Communications and Network, 2016, 8, 57-66
Published Online May 2016 in SciRes. http://www.scirp.org/journal/cn
http://dx.doi.org/10.4236/cn.2016.82007

Colluding Jamming Attack on a Grand Coalition by Aggrieved Nodes

Ashraf Al Sharah, Taiwo Oyedare, Sachin Shetty

Department of Electrical and Computer Engineering, Tennessee State University, Nashville, TN, USA
Email: aalshara@my.tnstate.edu, toyedare@my.tnstate.edu, sshetty@tnstate.edu

Received 3 March 2016; accepted 28 March 2016; published 31 March 2016

Abstract

Mobile Ad-Hoc Networks (MANETs) are highly vulnerable to insider jamming attacks. Several approaches to detect insider jammers in MANET have been proposed. However, once the insider jammer is detected and removed from the network, it is possible for the insider jammer to leverage the knowledge of insider information to launch a future attack. In this paper, we focus on collaborative smart jamming attacks, where the attackers who have been detected as insider jammers in a MANET, return to attack the MANET based on the knowledge learned. The MANET uses a reputation-based coalition game to detect insider jammers. In the collaborative smart jamming attack, two or more smart jammers will form a coalition to attack the coalitions in the MANET. The smart jammers were detected and then excluded from their initial coalition, they then regrouped to start their own coalition and share previously gained knowledge about legitimate nodes in their erstwhile coalition with the aim of achieving a highly coordinated successful jamming attack on the legitimate coalition. The success of the attack largely depends on the insider jammer's collective knowledge about the MANET. We present a technique to appropriately represent knowledge gathered by insider jammers which would lead to a successful attack. Simulation results in NS2 depict that coalition of jammers can leverage past knowledge to successfully attack MANET.

Keywords

MANETs, Jamming-Attacks, Coalition, Experience, Accuracy, Knowledge, Transmission-Rates

1. Introduction

In recent times, techniques to defend against threats in Mobile ad hoc networks (MANET) have received lots of attention. Insider threats in MANET have gained lots of traction. Insider nodes in MANET are hard to detect due to the unpredictability associated with their malicious intentions. For example, the insider nodes typically

How to cite this paper: Al Sharah, A., Oyedare, T. and Shetty, S. (2016) Colluding Jamming Attack on a Grand Coalition by Aggrieved Nodes. *Communications and Network*, **8**, 57-66. http://dx.doi.org/10.4236/cn.2016.82007

depend on accumulating knowledge about network topology and transmission rates in MANET to gain operational insight prior to launching an attack. Armed with detailed knowledge of network topology, routing patterns, identification of critical nodes, the insider threats selectively target critical network functions. The attack on critical network functions will impair the ability of legitimate nodes to communicate securely.

In a prior effort, we have proposed a reputation-based coalition game to detect insider threats in MANET [1]; in our approach, we proposed the formation of a grand coalition which will detect insider threats based on stored transmission rate and reputation for each node in the coalition. However, after an insider node is detected and removed from the coalition, it is possible for a group of insider nodes to collaborate and form an attack coalition and attempt to attack the original grand coalition. If an attacker node is successful in joining the attacker coalition, it improves the probability of successful cooperative jamming attack on the legitimate nodes' grand coalition.

Several types of collaborative/cooperative attacks on MANETs have been studied in literature [2]-[7]. The most common collaborative insider attacks include blackhole, wormhole and Sybil attacks. Blackhole attacks occur when a malicious node announces itself as having the best route to nodes whose packet it seeks to obstruct [8]. Once such a node locates itself between communicating nodes, it has the ability to alter the packets passing between them. Wormhole attacks occur when a malicious node receives packets and then sends that packet to another malicious node in the network [9]. Wormhole attacks involve the collaboration of two or more malicious nodes in the network. Sybil attacks occur when a malicious node generates additional nodes with fake identities. The ability of the attacker to act as different identities breaches the defense mechanism of the network. The collaborative attacks studied previously required that the nodes remain in the network while they carry out their attack, our work presents a new type of attack which is launched by a coalition of disgruntled node that has been excluded from the original coalition.

In this paper, we present an attack technique which involves a collaborative attack by a coalition of disgruntled nodes on a legitimate coalition in a MANET. In the rest of the paper, disgruntled nodes referred to the set of insider nodes which were detected and moved out of the grand coalition in the MANET. The disgruntled nodes form an attack coalition with the intent to join the grand coalition and launch cooperative jamming attacks on the MANET. The success of the attack depends on the accurate knowledge of the network topology and transmission rates.

2. Related Work

There have been several efforts on protecting MANETs against collaborative attacks. Gong *et al.* [10] discussed the security problem of cooperative immunization against collaborative attacks such as Blackhole attacks and wormhole attacks in MANETs such as worldwide interoperability for Microwave Access (WiMAX) networks. They proposed a tri-tier cooperative immune model to detect and eliminate collaborative attacks in MANETs. Their work focuses majorly on attacks perpetrated by nodes that are a part of the network. They differ from our work in the sense that they do not consider the attackers as former insiders but the attackers still partake in the network activities.

Wang *et al.* [11], obtained spectrum availability rates analytically, in particular, they considered that the jammers collaboratively apply sweeping attack to jam the channels at the base station side and the user side. They also proposed a collaborative defense strategy where users form tiers to exploit the temporal and spatial diversity to avoid jamming [11]. They have implemented their work only in cognitive radio networks and there is no certainty that their result could be achieved in a mobile ad-hoc network like ours.

Viet *et al.* [12] also addressed the problem of collaborative insider attacks, where two or more insiders work together work together to compromise critical data in information systems. They discuss the relations among system components which can be exploited by insiders, they focus on detecting malicious information flow through bridge data items [12]. They have only been able to show an attack launched by insiders who still have access to the network, there is no indication of excluding such attackers from the system and consequently preventing them from re-entering the system. Our approach differs in that we model excluded insider jammers who collaborate in order to disrupt network activities in the previous coalition they belong to.

3. System Model

Our system model consists of the legitimate grand coalition and attacker coalition (**Table 1**, **Figure 1**). The legitimate

Table 1. A summary of notations.

Symbol	Definition
R	Transmission rates
j_N	Number of smart jammers
C	Nodes in the rival coalition
C_j	A node, *j*, in the rival coalition
S	Nodes in the legitimate coalition
$K_t(C_j)$	Knowledge gained by rival coalition nodes
P_{ji}	Probability of knowledge gained from node *i* by node *j*
x_tC_j	Payoff for nodes in the rival coalition
O	Observations
T	Total time attacker spend in the legitimate coalition
E_j	Experience of a given node
A_j	Node knowledge accuracy
O_v	Overlapping rates
O_{vj}	Overlapping rates for node *j*
U_{ov}	Updated overlapping rate
U_{ovj}	Updated overlapping rate for node *j*

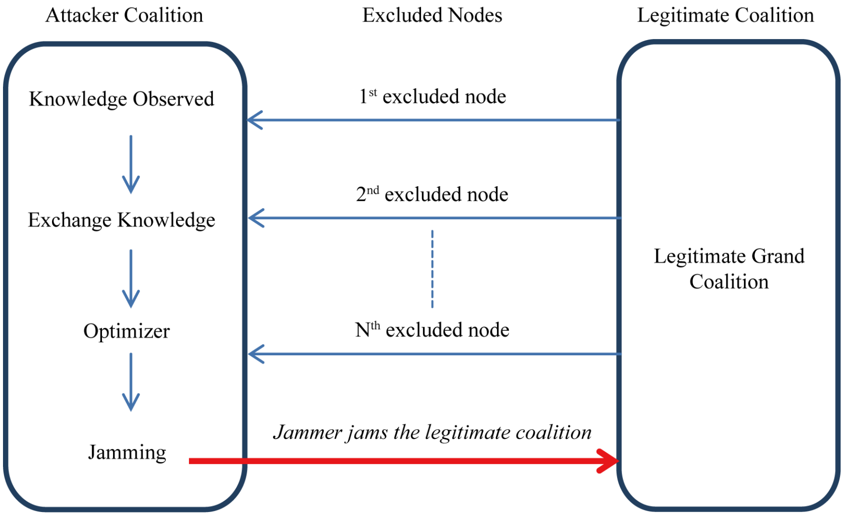

Figure 1. Collaborative attack system model.

grand coalition is designed to detect insider nodes in a MANET. However, the legitimate coalition can also be an attack surface which can be potentially targeted by insider nodes which have been detected and excluded.

The attacker coalition consists of excluded insider nodes, where j_N is number of smart jammers and $j_N = [j_1, j_2, \cdots, j_n]$. Each of the excluded jammer maintains a knowledge table called jammer knowledge table. This table keeps an updated record of the knowledge gained by the smart jammers in their previous coalition. The jammers would share this knowledge with other jammer in their new coalition. The knowledge table also consist the transmission rates gain by the attacker node during time, R, (where $R = [R_1, R_2, \cdots, R_n]$ rates).

3.1. Legitimate Grand Coalition Model

Nodes in the legitimate coalition rely heavily on a stored transmission rate table according to [13] and a reputation table for each individual node in the coalition. This mechanism will depend on storing these two tables in each node to define the internal attacker, which was an erstwhile legitimate node. The nodes will form as table grand coalition in order to make a strategic security defense decision, maintain the grand coalition by building and updating a reputation table according to the transmission rate table in all nodes and then exclude any malicious node that has a reputation value below the threshold value. Each node will have a reputation table for all neighboring nodes. Our previous effort in [1] explains more about the legitimate grand coalition model.

3.2. Attacker Model

3.2.1. Attack Surface

As stated in the beginning of the system model, the attack surface is the legitimate coalition which consists of any number of nodes. The nodes could range from a legitimate node to an insider jammer node that has not been identified. From our previous work, the insider jammers are excluded in a consecutive manner. The nodes left in the legitimate coalition after the exclusion of the jammers would be the attack surface. The legitimate coalition change their communication mechanism after a jammer node has been excluded by hopping between the transmission rates.

3.2.2. Attackers' Coalition Formation

Throughout this paper, we refer to the attacker's coalition as rival coalition. The main goal of forming a rival coalition is to ensure that the excluded nodes focus on a more assured jamming success rather than just jamming blindly or randomly. When the first node was excluded, some changes were made by the coalition about the channel of communication, this information is unknown to the first node, but the information can be provided by the second excluded node. This information helps in identifying the pattern of transmission rate hopping used after a malicious node has been excluded.

The attackers share the knowledge they gathered in the legitimate coalition. Based on the knowledge gathered, the attackers form a rival coalition with similar pattern of the coalition formation of the legitimate coalition. This rival coalition has more chances of achieving their goal of a successful jamming attack with lesser effort.

Any node that seeks to join rival coalition should meet the criteria for admittance. The criteria for admittance are that such a node should have the knowledge of at least ten nodes who belong to the legitimate coalition.

$$K_t\left(C_j\right)=\frac{\sum_{i\in S} p_{ij}}{|S|}\Bigg| S\geq 10\,. \tag{1}$$

From Equation (1), *S* can be used as a varying factor to increase the difficulty of gaining entry into the rival coalition. If the node fails to meet this criterion, it will be denied acceptance.

The payoff of the nodes when they join the rival coalition is shown in Equation (2).

$$x_t\left(C\right)=\frac{1}{|C|}\left(K_t\left(C\right)\right). \tag{2}$$

The coalition formation process starts when the first malicious node is excluded from the legitimate coalition. This node becomes the first member of the rival coalition. It starts to broadcast a forming option after it has been excluded in order to find a matching partner to begin the coalition with. The second excluded node would get the broadcast message and would accept the forming option accompanying the broadcast message. After accepting the forming option, they form their own coalition. The coalition formation process is continued iteratively for all other excluded nodes, they all get the broadcast message once they have been excluded. The excluded nodes stand to benefit from the knowledge shared by the other excluded nodes. The excluded nodes have the option of not joining the coalition as they could choose to launch an attack on their own, as we would see in our results section, the jammers achieve little success in this regard when compared with the impact they would make if they form a coalition.

In the rival coalition, nodes will share their previous knowledge table with each other in order to pick the best transmission rate to start with. This sharing of knowledge continues even when a new node joins the rival coalition.

Algorithm 1. Attackers Coalition formation algorithm

```
FOR $T = t_0 : t_n$
First excluded node $j_1$, starts broadcasting a forming signal
if matching found $C \geq 2$ then
C exist,
        Exchange $K_t(C_j)$ and keep broadcasting
else
        C does not exist
        keep broadcasting
end if
end FOR
```

3.2.3. Optimization of Knowledge Gained

We form the rival coalition based on the previous knowledge gained by nodes during different times, for example j_1 gained knowledge between t_3-t_{15} and j_3 gained knowledge between t_{11}-t_{20}, therefore, we will need to optimize the knowledge since it was collected at different times by different nodes with a time overlap between them. The optimization strategy is that each node will create an overlapping transmission rate table, O_v (where $O_v = [O_{v1}, O_{v2}, \cdots, O_{vn}]$), which will contain the common rates observed by the majority of nodes, after creating this table, another optimization is done based on the nodes' accuracy and experience, this two factors are necessary in order to extract the most accurate information from the knowledge table to create the attackers' knowledge table.

Experience is defined as the amount of knowledge gained by an attacker node during the time spent in the legitimate coalition. Experience is also defined by an attacker nodes understanding of the different defense mechanisms employed by the legitimate node after the exclusion of any jammer node. Such mechanism could involve the attackers understanding of how the nodes in the original coalition hop between transmission rates after an attack.

Accuracy is defined by the testimony of the freshest node that joins the rival coalition, where such a node confirms the defense mechanism used or the change of strategy by the legitimate coalition or new node knowledge in the legitimate coalition. The accuracy component shows that the latest node to be excluded from the coalition would have the most updated knowledge about the network.

The testimony of both an excluded expert node and the newest entrant to the rival coalition should satisfy the usage of those rates. If this occurs, these rates would be retained in the table otherwise, it will be discarded.

The last step in the optimization will be the rearrangement of the transmission rates according to the frequency of their usage between two nodes. If the majority of the nodes report a rate to be highly used, then it should get the highest priority, if not its priority will be low.

We define the attacker coalition nodes experience as knowledge graph with respect to observations according to time. Figure 2 will show this process.

We defined O as a set of observations of transmission rates R at specific time for an attacker node during its stay in the legitimate coalition where $O = o_1(t), o_2(t), \cdots, o_n(t)$ and T is the total time which the attacker node spent in the legitimate coalition where $T = 0, 1, \cdots, t$, by gaining different amount of observations we will have nodes with different levels of experience. To identify the experienced node we depend on the knowledge graph to identify a trustworthy node.

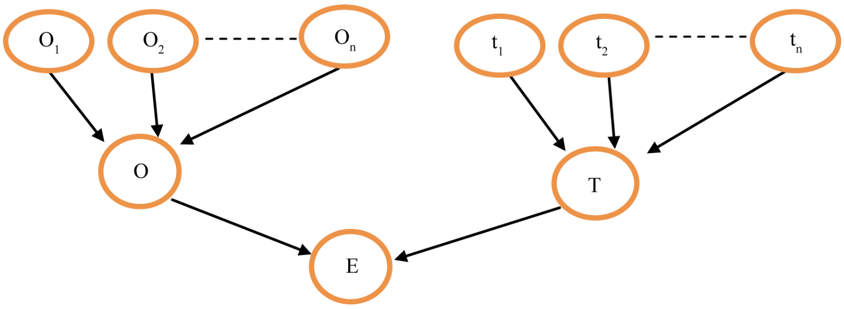

Figure 2. Knowledge graph for node's experience.

$$E_j = \max\{O_t(T)\}. \tag{3}$$

The other factor for updating the attacking table is accuracy, as explained, this factor checks if a fresh node has a non-existent knowledge about the legitimate coalition. Algorithm 2 is used to check a node's accuracy.

Algorithm 2. Algorithm for defining Accuracy

```
FOR $T = t_0 : t_n$
    if $j_n \subset C$ then
if $j_n \in$ new $K_t(C_j)$ then
    $j_n \subset A$, go to algorithm 3
else
    $j_n \not\subset A$
end if
end if
end FOR
```

3.2.4. Jamming Attack Strategy

We consider our smart jamming attack as a sweep jammer where jammers can sweep through the transmission rates. The jamming strategy is explained in this section. After the nodes form the rival coalition and share their knowledge tables, they choose which of the nodes in the legitimate coalition to attack based on the optimized knowledge (explained in 3.2.3). We do not follow a random selection because this will consume too much power and may not result in a successful attack. After the knowledge has been shared, an overlapped transmission rate table will be generated. The overlapped rates table contains transmission rates that are common for many nodes in the legitimate coalition. The importance of the overlapped rates table is to optimize the transmission rates values; consequently, overlapping rates can be eliminated based on the accuracy and experience of each of the excluded nodes. Steps for creating the overlapped rates:

- After sharing the knowledge tables, find the overlapping transmission rates.
- Store the overlapping rates in an overlapping rate table contained in all nodes.
- If the overlapping rates are found in E_j and A_j nodes then keep it else eliminate.
- Rearrange the overlapped table according to the new outputs.

Algorithm 3. Attack Algorithm

```
FOR $j_N = j_1 : j_n$
Create $O_v$ where $O_v \in R$
if $O_{vj} \in (E_j \& A_j)$ nodes then
Move $O_{vj}$ to highest attacking probability
Create $U_{ov}$ table to attack
end if
end FOR
FOR all $U_{ov}$
Select most probable $U_{ovj}$ rate to attack
end FOR
```

4. Simulation and Results

We implemented our approach using NS2 simulator. Without loss of generality, the attack surface will consist of 40 with 8 insider attacks. This simulation will show different sizes of jammers coalition (4, 5, 6, 7, 8) to show how more nodes we have in the coalition more improvement we get in the results. Furthermore, we show the impact of the jamming attack while the rival coalition size increases. The number of generated and successful attacks comparing five different rival coalition sizes is also shown. There would also be a comparison between the importance of updating the transmission rate overlap table and not updating as well. In addition, we show the strength of our method compared with isolated attacks for multiple attackers where those nodes do not form a coalition. Finally, we will show the time taken from each rival coalition size to perform the first successful attack.

4.1. Jamming Impact

Figure 3 shows the jamming impact for the presented method with different rival coalition size, it can be seen that as the rival coalition size grew, the impact increases sharply that is because the rival coalition has more information about the original coalition from different jammers in different locations inside the original coalition which gives them more impacting power. For the rival coalition of 8 jammer nodes, the impact of jamming is increased significantly; this shows that having more jammer nodes in the rival coalition would give a higher jamming impact.

4.2. Number of Generated Attacks

Figure 4 shows the number of attacks carried out by different jammers coalition sizes, it can be seen that more nodes we have in the coalition more attacks will be generated during time. The highest number of attack is generated by the 8-jammers rival coalition. This is because the jammer nodes have more resources to properly generate an attack. This generated attack is not to be confused with a successful attack, as would be seen in the next result. A generated attack comprises of both successful and unsuccessful attacks launched by the rival coalition. Given the same amount of time, the number of attacks generated by the 8-jammers coalition almost triples the 4-jammers coalition as shown in **Figure 4**. The relationship between these rival coalition size and the number of attacks generated is not linear because as the time increases, the addition of one extra node could jerk up the number of generated attacks in an unprecedented manner.

4.3. Number of Successful Attacks

Figure 5 shows how many successful attacks have been accomplished from the total generated attacks shown in **Figure 4**. A successful attack is defined by the extent of damage done to any link between two or more legitimate

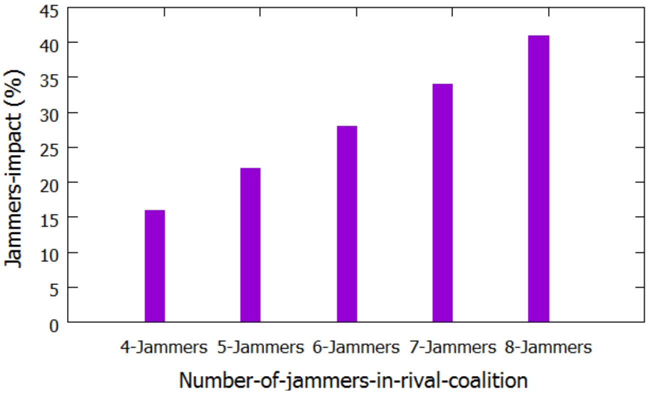

Figure 3. Jammer impact with different rival coalition sizes.

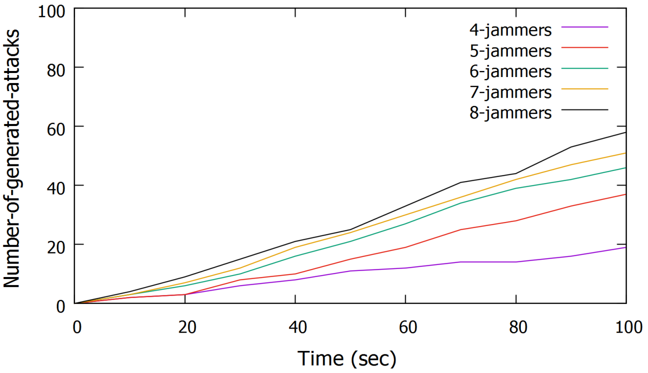

Figure 4. Comparing number of generated attacks with different rival coalition sizes.

nodes in the original coalition. As expected, not all the generated attack was successful, but we could see that the 8-jammers rival coalition still has the highest successful attacks. For the 8-jammers rival coalition, the number of successful attack is about eighty-three percent of the generated attack shown in **Figure 4**. The other coalition size has similar performance increment.

4.4. Percentage of Accuracy

Figure 6 shows the comparison between using and not using the updated overlapping table. The updated overlapping table is used based on experience of the nodes and the testimony of the newest entrant node to the rival coalition. When the overlapping table is not used, the accuracy of the shared information is considerably reduced. In **Figure 6**, the difference between the percentages of accuracy for the 8-jammer coalition is significantly greater than the difference in the accuracy of the 4-jammer coalition.

4.5. Coalition versus Non-Coalition for Excluded Nodes

Figure 7 shows the benefit of forming a rival attacker coalition method over each jammer attacking independently through information they gathered from the original coalition. We show that when the excluded nodes do not form a coalition, their jamming accuracy is significantly different from when they do form a coalition.

4.6. Time Taken for First Successful Attack

Figure 8 shows the time taken for different jammers coalition sizes to accomplish the first successful attack, and it can be seen that the more attackers we have, the quicker they can launch a successful attack. The first successful attack is the first successful generated attack. As the coalition size reduces it takes a longer time to ensure that the attacks generated are successful.

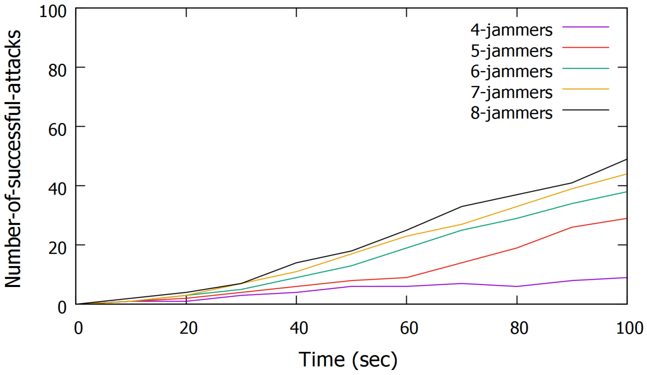

Figure 5. Comparing number of successful attacks with different rival coalition sizes.

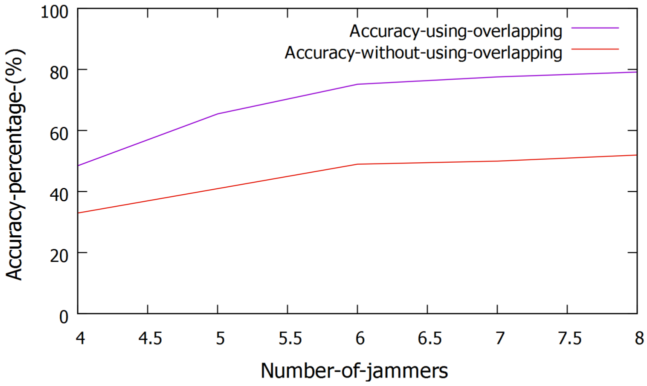

Figure 6. Accuracy percentage.

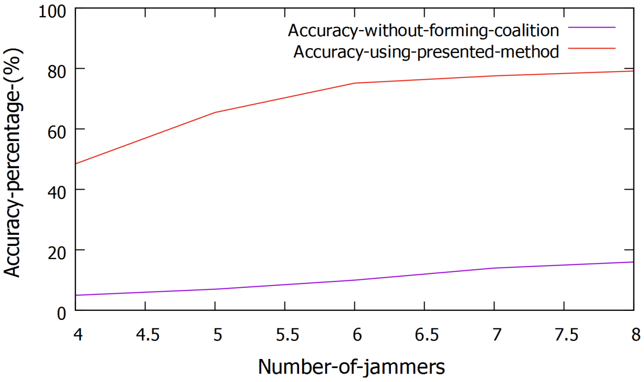

Figure 7. Coalition approach versus isolated approach for excluded nodes.

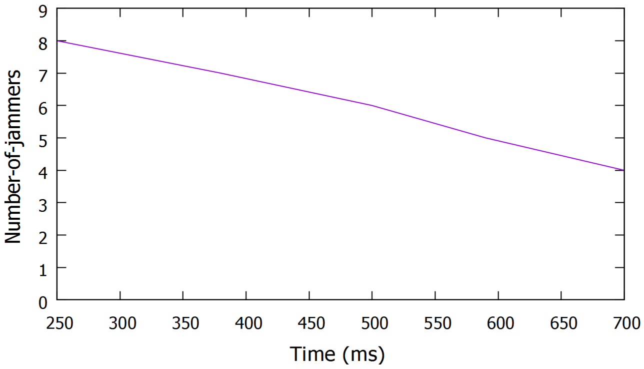

Figure 8. Time taken from different coalition sizes to achieve the first successful attack.

5. Conclusion and Future Works

In this paper, we showed that jammer nodes that were excluded from a coalition could form a rival coalition of their own in order to attack their previous coalition. The nodes attack the legitimate coalition based on two important factors namely: accuracy and experience. The legitimate coalition becomes the attack surface for the rival coalition. An algorithm for the attack was created and we were able to show from our result the impact of the jamming launched by the rival coalition. In addition, the number of generated attack given the use of accuracy and experience was also shown. From our results, the percentage of successful attacks to the generated attacks was high when compared with isolated attacks. In the future, we will like to see how this type of attack can be mitigated by the legitimate coalition. One way by which this can be done is through the use of baits to lure the attackers away from the rival coalition.

Acknowledgements

This work is supported by Office of the Assistant Secretary of Defense for Research and Engineering agreement FAB750-15-2-0120, NSF CNS-1405681, and DHS 2014-ST-062-000059.

References

[1] Oyedare, T., Al Sharah, T. and Shetty, S. (2016) A Reputation-Based Coalition Game to Prevent Smart Insider Jamming Attacks in MANETs. *International Conference on Wired/Wireless Internet Communications* (*WWIC*), Thessaloniki, 25-27 May 2016.

[2] Chen, M.-H., Lin, M.-H., Hong, Y.-W.P. and Zhou, X. (2013) On Cooperative and Malicious Behaviors in Multirelay Fading Channels. *IEEE Transactions on Information Forensics and Security*, **8**, 1126-1139.
http://dx.doi.org/10.1109/TIFS.2013.2262941

[3] Long, H., Wei, X.G., Zhang, X., Wang, J. and Wang, W. (2014) Cooperative Jamming and Power Allocation in Three-Phase Two-Way Relaying System with Untrusty Relay Node. 2014 *XXXIth URSI General Assembly and Scientific Symposium* (*URSI GASS*), Beijing, 16-23 August 2014, 14.

[4] Dong, L., Zadeh, H.Y. and Jafarkhani, H. (2011) Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper. 2011 *IEEE International Conference on Communications* (*ICC*), Kyoto, 5-9 June 2011, 15.

[5] Yang, J., Kim, I.-M. and Kim, I.-M. (2013) Optimal Cooperative Jamming for Multiuser Broadcast Channel with Multiple Eavesdroppers. *IEEE Transactions on Wireless Communications*, **12**, 2840-2852. http://dx.doi.org/10.1109/TWC.2013.040413.120972

[6] Zhang, Q., Huang, X., Li, Q. and Qin, J. (2015) Cooperative Jamming Aided Robust Secure Transmission for Wireless Information and Power Transfer in Miso Channels. *IEEE Transactions on Communications*, **63**, 906-915. http://dx.doi.org/10.1109/TCOMM.2015.2405063

[7] Yang, J., Kim, I.-M. and Kim, D.I. (2014) Joint Design of Optimal Cooperative Jamming and Power Allocation for Linear Precoding. *IEEE Transactions on Communications*, **62**, 3285-3298. http://dx.doi.org/10.1109/TCOMM.2014.2345659

[8] Gagandeep, A. and Kumar, P. (2012) Analysis of Different Security Attacks in MANETs on Protocol Stack: A Review, *International Journal of Engineering and Advanced Technology* (*IJEAT*), **1**, 22-49.

[9] Stanojev, I. and Yener, A. (2011) Recruiting Multi-Antenna Transmitters as Cooperative Jammers: An Auction-Theoretic Approach. 2011 49*th Annual Allerton Conference on Communication*, *Control*, *and Computing*, Monticello, IL, 28-30 September 2011, 1106-1112.

[10] Gong, T. and Bhargava, B. (2013) Immunizing Mobile ad Hoc Networks against Collaborative Attacks Using Cooperative Immune Model. *Security and Communication Networks*, **6**, 58-68. http://dx.doi.org/10.1002/sec.530

[11] Wang, W., Bhattacharjee, S., Chatterjee, M. and Kwiat, K. (2013) Collaborative Jamming and Collaborative Defense in Cognitive Radio Networks. *Pervasive and Mobile Computing*, **9**, 572-587. http://dx.doi.org/10.1016/j.pmcj.2012.06.008

[12] Viet, K., Panda, B. and Hu, Y. (2012) Detecting Collaborative Insider Attacks in Information Systems. 2012 *IEEE International Conference on Systems*, *Man*, *and Cybernetics* (*SMC*), Seoul, 14-17 October 2012, 502-507.

[13] Al Sharah, A. and Shetty, S. (2015) Accumulative Feedback Adaptation Transmission Rate in Mobile Ad-Hoc Networks. 2015 *International Conference and Workshop on Computing and Communication* (*IEMCON*), 15-17 October 2015, Vancouver, 15.